Allied Telesis™

Allied Telesis provides advanced edge security

for enterprise networks

Solutions | Network Access Control (NAC)

The security issues facing enterprise networks have evolved over the years, with the focus moving from mitigating outward attacks to reducing internal breaches and the infiltration of malicious software. This internal defence requires significant involvement with individual devices on a network, which creates greater overhead on network administrators. Allied Telesis lower this overhead and provide an effective solution to internal network security by integrating advanced switching technology as a part of Network Access Control (NAC).

The evolution of network defences

For many years, the focus in enterprise network security was on defending against external threats. Firewalls were installed to protect the LAN from the hackers, worms, and spammers 'out there' in the lawless land of the Internet.

However, with the growth in mobile computing and the proliferation of Ethernet-capable devices, LAN-based attacks now outnumber external threats as the main security issues facing network administrators. Attention has turned towards the enemy within.

Malicious software, known as malware, makes its way onto a network through employees, contractors, and visitors. Their laptops, wireless gadgets, and ever popular USB flash drives all provide excellent vectors through which malware can enter the workplace. Even careful employees can unwittingly bring in malware after using their equipment outside of the network. Visitors and contractors may be careless carriers of malware or, even worse, may be planning a malicious attack to steal data or cause disruption.

Defence against the enemy within

To effectively defend the network against internal threats, network administrators need secure LAN switches that provide protection against common attacks. They also need to implement policies that ensure that each device connecting to a network is as secure as possible. This combination of secure LAN switches and anti-malware policy can be very effective.

For some time now, Allied Telesis switches have provided a suite of defenses to combat internal attacks. These range from data stealing attacks such as ARP spoofing, to Denial of Service attacks such as Tear Drop or Ping of Death. Correct deployment of these defenses can create a network that is impermeable to most of the harm from these attacks.

More detailed information on how Allied Telesis secure LAN switches defend against the various types of LAN threats can be found on our website.

http://www.alliedtelesis.com/solutions/category.aspx?5

Additionally, network administrators can institute a policy whereby network users are required to install and maintain anti-malware scanners, and to install security patches as they are released by Operating System vendors. However, this has required network administrators to spend time ensuring that users are adhering to policies, and even generated counter-productive tension between network administrators and the users.

This is where Network Access Control (NAC) provides a solution. NAC allows network administrators to automate policy enforcement - rather than requesting that users ensure their devices conform to anti-malware policies, let the network do the job instead.

Network Access Control has very quickly become an industry requirement and much more than a new buzzword for network professionals. NAC offers an excellent way to control network access with automated policy enforcement, and manage network security without vast administration overhead.

NAC controls network access and security with a minimum of staff overhead.

Put simply, NAC enables you to define a comprehensive security policy for your network, implement that policy on a centralized server, and have the network automatically enforce that policy on all network users. NAC is much more than just user authentication, it is also designed to protect the network from users and devices that may be authorised, but pose other threats. The most sensible place for this to occur is at the edge of the network, removing security threats before they gain any form of access. A NAC solution including switches that act as enforcement points ensures a proactive approach to network security.

How NAC secures your network

Nowadays, network access for multiple device types or temporary users is an expectation, not an exception. With this in mind, today's enterprise network requirements include:

- Some level of access no matter who or where you are
- Access for guests such as sub-contractors, partners, remote employees
- Access control for a new range of network devices, such as iPhone and BlackBerry devices, PDAs and digital cameras

Allied Telesis LAN switches meet these emerging requirements with NAC features and integration. Used in conjunction with appropriate server-side and client-side software tools, they can provide a remarkable level of control over the security status of the devices that connect to your network. Allied Telesis NAC implementation is TCG/TNC (Trusted Computing Group - Trusted Network Connect) standards-based to guarantee interoperability with the major third party suppliers of NAC software, such as Microsoft and Symantec. This provides customers with the confidence to create a comprehensive NAC solution from trusted vendors.

At the heart of using NAC for your network security are three key elements:

- No (or very limited) access without identification
- The quarantine and remediation of non-compliant devices
- Setting the level of access to network resources based on a device's authenticated identity

Solutions | Network Access Control (NAC)

In practice, this means that every device is required to identify itself when it connects, and if appropriate be examined for its compliance to security policies. On a typical network, devices that:

- cannot provide a valid identity are completely barred from the network (or alternatively could have restricted access to the Internet, and nothing else)
- authenticate successfully but fail the policy adherence test are given access to a remediation process, and nothing else
- authenticate successfully and are deemed policy adherent are given access to the network resources that match their identity

This layered approach to network access control is illustrated in figure 1.

In this way, security policy enforcement and resource access control are performed by the network itself, utilizing NAC. Malware cannot harm the network, as it is never allowed access to the network. Intruders cannot commit theft or cause disruption, as they are either blocked or very tightly constrained.

NAC features on Allied Telesis switches

To provide this advance in network security, the significant elements included in Allied Telesis switch functionality are Tri-authentication and NAC integration with third-party software.

Tri-authentication

Tri-authentication allows the network to identify all devices connecting to it. It can be used as part of a comprehensive NAC solution; or on its own provides a low overhead method of implementing network access security.

The three authentication methods, as illustrated in figure 2, are:

- 802.1X authentication
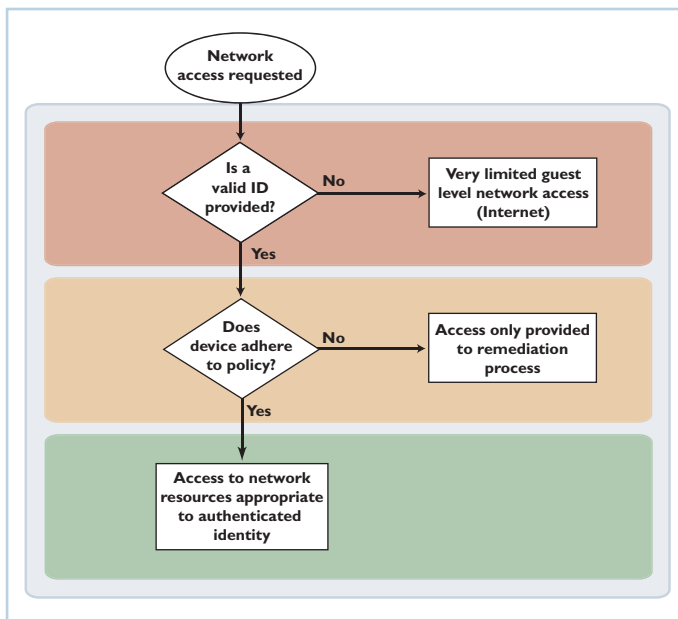- Web-based authentication
- MAC authentication

Figure 1: Network Access Control (NAC)

802.X is a highly secure authentication protocol that enables encrypted password exchange and certificate validation. A user is prompted for their name and password, and this is then checked against a user database before they are able to access the network. It is secure and configurable, but does require that 802.1X software is embedded and also configured in the client device. Not all devices connecting to the network will have this software embedded or pre-configured - this is particularly so for users who are temporary visitors.

Web authentication is provided to cater for computers in which 802.1X is not present or configured. The switch detects web-browsing activity from the client computer, and presents a login screen to the web browser. The user can progress no further until they have submitted a valid identity using the login screen. This authentication can either be performed in clear text, using the HTTP protocol, or performed in encrypted form using the HTTPS protocol.

MAC authentication is a fallback option you can use for non-interactive devices like printers or web cameras. The device's MAC address provides a unique identity that can be used to authenticate the device.

By providing these three authentication options, the Allied Telesis switches make it possible to build a network in which you can authenticate all devices attaching to the network.
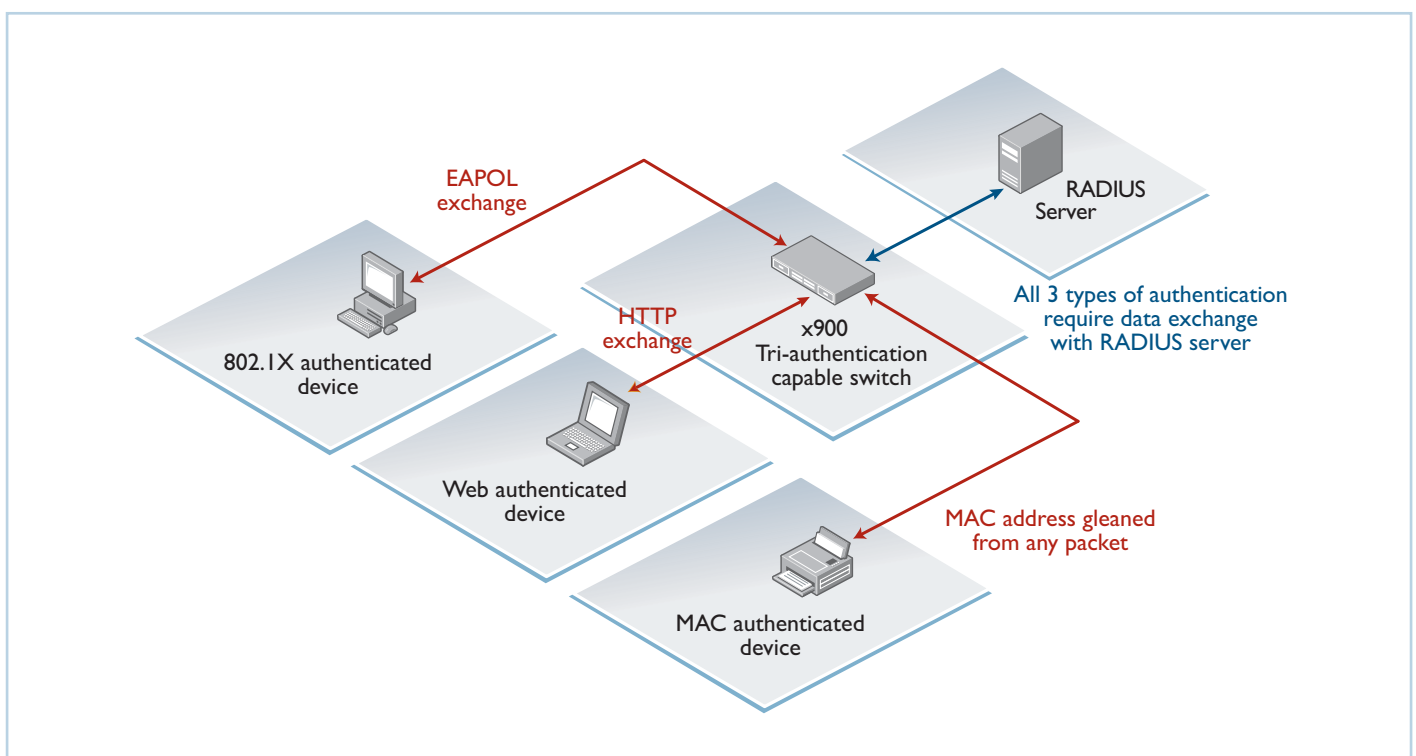

EAPOL
exchange

RADIUS
Server

All 3 types of authentication
require data exchange
with RADIUS server

802.1X authenticated
device

HTTP
exchange

x900
Tri-authentication
capable switch

Web authenticated
device

MAC address gleaned
from any packet

MAC authenticated
device

Figure 2: Tri-authentication

Integration with NAC Infrastructures

NAC integration makes it possible for the switches to act in the role of enforcement point in a NAC infrastructure with third party software vendors. Specifically, this means that the switch will:

- transport the packets that constitute the NAC server's interrogation of the client device
- receive notification of the decision made at the decision point, and enforce that decision

Figure 3 illustrates the role of the switch as Policy Enforcement Point (PEP) in a NAC solution.

The NAC server decides the level of network access a user can have, or any remedial action required to bring the user's computer (or other end-point) up to an acceptable level of compliance. The switch acts as the policy's enforcer, ensuring the ongoing security of the network and access to resources for users as appropriate. The Integration of advanced switching technology in a NAC solution provides very granular enforcement options, providing significant added value to the NAC infrastructure.

A more secure network

In conclusion, the modern enterprise has seen a phenomenal increase in the convergence of functionality on the network with voice, video, security monitoring and more added to the traditional data and internet access. The need to control network access and provide a secure infrastructure is greater than ever.

Network Access Control can mitigate threats by combining access control with automated management of the security compliance of devices attached to the network. The advanced edge features on Allied Telesis switches ensure a secure environment for business to thrive.
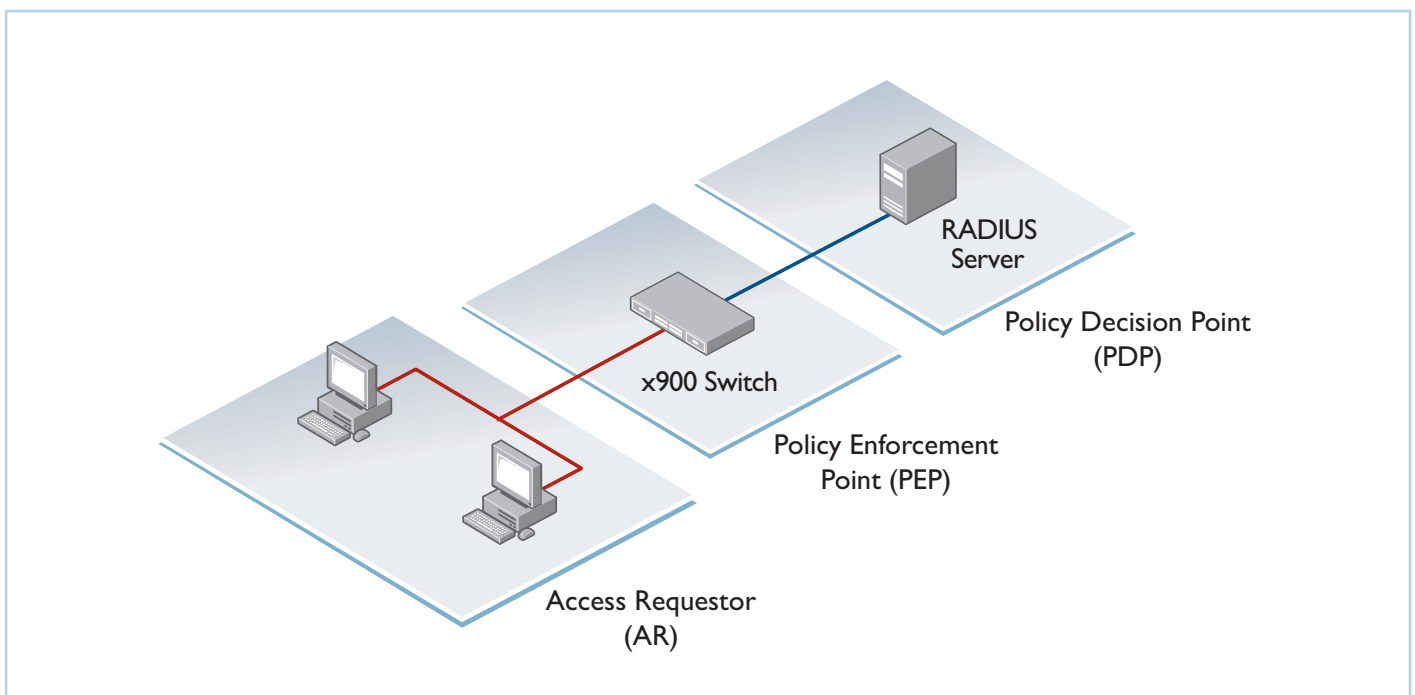
RADIUS
Server

Policy Decision Point
(PDP)

x900 Switch

Policy Enforcement
Point (PEP)

Access Requestor
(AR)

Figure 3: NAC Integration

Products

The following Allied Telesis advanced switching products support NAC.* Further products will have NAC capability integrated in the near future.

SwitchBlade® x908

SwitchBlade x908

Advanced Layer 3 Modular Switch
- 8 x 60Gbps Expansion Bays

x900 Family

x900 Family

x900-12X and 24X Series

Advanced Gigabit Layer 3+ Expandable Switches

x900-24XT
- 2 x 60Gbps Expansion Bays
- 24 x 10/100/1000BASE-T (RJ-45) copper ports

x900-24XT-N
NEBS Compliant
- 2 x 60Gbps Expansion Bays
- 24 x 10/100/1000BASE-T (RJ-45) copper ports

x900-24XS
- 2 x 60Gbps Expansion Bays
- 24 x 100/1000BASE-X SFP ports

x900-12XT/S
- 1 x 60Gbps Expansion Bay
- 12 x combo ports (10/100/1000BASE-T copper or SFP)

x900-48 Series

Enhanced Fast Ethernet Layer 3+ Switches

x900-48FE
- 48 x 10/100BASE-T copper ports
- 4 x 1000BASE-X SFP uplinks

x900-48FS
- 48 x 100BASE-X SFP ports (Fiber only)
- 4 x 1000BASE-X SFP uplinks

AT-9900 series

Multilayer IPv4 and IPv6 Gigabit switches

AT-9900 Series

AT-9924T

■ 24 x 10/100/1000BASE-T copper ports

■ 4 x 1000BASE-X SFP combo ports

AT-9924SP

■ 24 x 100/1000BASE-X SFP ports

AT-9400 series

Gigabit Ethernet Layer 3 Switches

AT-9424TS

AT-9424T

■ Layer 3 managed switch with 20 x 10/100/1000Base-T ports

■ 4 x 10/100/1000 / SFP combo ports

AT-9424Ts

■ Layer 3 stackable switch with 20 x 10/100/1000Base-T ports

■ 4 x 10/100/1000 / SFP combo ports

AT-9424Ts/XP

■ Layer 3 stackable switch with 20 x 10/100/1000Base-T ports

■ 4 x 10/100/1000 / SFP combo ports plus 2 x XFP bays

AT-9448T/SP

■ Layer 3 switch with 48 x 10/100/1000Base-T ports

■ 4 x SFP bays

AT-9448Ts/XP

■ Layer 3 stackable switch with 48 x10/100/1000Base-T ports

■ 2 x XFP bays

AT-9408LC/SP

■ Layer 2+ switch with 8-port 1000Base-SX (LC connectors)

■ 4 x SFPs plus memory flash card slot

AT8600 series

Layer 3 Fast Ethernet Switches

AT-8600 Series

AT-8624T/2M

■ 24 x 10/100BASE-T ports

■ 2 x Uplink Module Bays

AT-8648T/2SP

■ 48 x 10/100BASE-T ports

■ 2 x SFP ports in combo with 2 x 10/100/1000T uplink ports (RJ-45)

AT-8624POE

- 24 x 10/100BASE-T ports with PoE
- 2 x Uplink Module Bays

AT8500 series

Layer 3 Fast Ethernet Switches

AT-8500 Series

AT-8524M

- 24 x 10/100TX ports
- 2 x Expansion Bays

AT-8524POE

- 24 x 10/100TX ports, Power over Ethernet
- 2 x Expansion Bays

AT-8550/GB

- 48 x 10/100TX ports
- 2 x active GBIC bays (unpopulated)
- 2 x standby 10/100/1000T ports (RJ-45)

AT-8550/SP

- 48 x 10/100TX ports
- 2 x active SFP bays (unpopulated)
- 2 x standby 10/100/1000T ports (RJ-45)

AT-8516F/SC

- 16 x 100FX (SC) ports
- 2 x Expansion Bays

About Allied Telesis Inc.

Allied Telesis is a world class leader in delivering IP/Ethernet network solutions to the global market place. We create innovative, standards-based IP networks that seamlessly connect you with voice, video and data services.

Enterprise customers can build complete end-to-end networking solutions through a single vendor, with core to edge technologies ranging from powerful 10 Gigabit Layer 3 switches right through to media converters.

Allied Telesis also offer a wide range of access, aggregation and backbone solutions for Service Providers. Our products range from industry leading media gateways which allow voice, video and data services to be delivered to the home and business, right through to high-end chassis-based platforms providing significant network infrastructure.

Allied Telesis' flexible service and support programs are tailored to meet a wide range of needs, and are designed to protect your Allied Telesis investment well into the future.

Visit us online at www.alliedtelesis.com

* Not all of the listed products support all NAC features as discussed. For details of which features are supported on a specific product, please refer to the Allied Telesis website for product documentation, or talk to your Allied Telesis reseller.

C618-31006-00 Rev. A

Connecting The (IP) World

Allied Telesis